The Claims Defining the Invention are as Follows

1. A security system for an operating system of a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and a read/writeable storage device for storing data to be handled by the computer, the security system, comprising:

a security partition formed in the storage device, wherein the operating system is stored in the security partition;

profiling means to define at least two different data access profiles with respect to the storage device for users of the computer, one access profile ascribing read/write access to data stored on said security partition, and the other access profile ascribing a blocking level of access that does not permit write access to said security partition; and

blocking means for selectively blocking data access between the host CPU and the security partition in accordance with the particular data access profile defined for a user effecting data access to the storage device at any particular point in time;

wherein said blocking means is independent and separately configurable of said host CPU to impose and continuously maintain the requisite level of data access to said security partition for users effecting said data access in accordance with the particular data access profile thereof regardless of the subsequent operations of the host CPU.

2. A security system as claimed in claim 1, including authentication means to authenticate a user of the computer having a prescribed data access profile and configure said blocking means to control subsequent access to the security partition in accordance with the data access profile of that user, before that user is able to access said security partition regardless of the particular data access profile of that user.

3. A security system as claimed in claim 2, wherein said blocking means includes processing means independent of the host CPU for controlling the operation of said blocking means in response to said authentication means.

4. A security system as claimed in claim 3, wherein said blocking means is configured to block all data access by the host CPU to the storage device before and during initialisation of the security system and includes intercepting means to intercept all said data access immediately after said initialisation and effect data access to the storage device and said security partition under the control of said processing means in accordance with the data access profile of users effecting said data access as authenticated by said authenticating means.

5. A security system as claimed in claim 4, wherein said processing means effects independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device, upon said intercepting means intercepting said data access immediately after said initialisation and before loading of the operating system of the computer.

6. A security system as claimed in claim 5, wherein said authentication means enables a software boot of the computer to be effected after correct authentication of the user, and said processing means permits normal loading of the operating system during the start up sequence of the computer following said software boot.

7. A security system as claimed in any one of the preceding claims, including memory store means independent of the memory means and the storage device of the computer to store critical data and control elements associated with the basic operation of the computer and access to the storage device.

8. A security system as claimed in claim 7, wherein said critical data and control elements are supplied to and used by the host CPU for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

9. A security system as claimed in any one of the preceding claims as dependent on claim 2, wherein the authentication means includes a login verifying means to enable a user of the computer to enter a login identification and password and have that login identification and password verified to authenticate said user being an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

10. A security system as claimed in claim 9, as further dependent on claim 7 or 8, wherein said login identification and passwords of authorised users and the prescribed data access profile thereof form part of said critical data and control elements and said login verifying means accesses said critical data and control elements to effect authentication of a user.

11. A security system as claimed in any one of the preceding claims, wherein the prescribed data access profile of a user comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions of the storage device, one of said prescribed partitions including said security partition.

12. A security system as claimed in any one of the preceding claims, wherein said blocking means is physically disposed in line with the data access channel between the host CPU and the storage device.

13. A security system as claimed in claim 12, wherein said blocking means is disposed as part of a bridging circuit effecting communications between the main data and control bus of the host CPU and the data access channel connected to the storage device.

14. A security system as claimed in claim 12, wherein said blocking means is disposed as part of a bridging circuit effecting communications between the data access channel and the storage device.

15. A security system as claimed in claim 12, wherein said blocking means is disposed intermediate the data access channel between the main data and control bus of the host CLU and the storage device.

16. A method for securing and protecting an operating system of a computer from unauthorised access, the computer having a host central processing unit (CPU), a read/writeable storage device for storing data to be handled by the computer, and memory used by the host CPU to load programs in order to operate the computer and storage device, the method comprising:-

forming a security partition in the storage device, and storing the operating system in the security partition;

defining at least two different data access profiles with respect to the storage device for users of the computer, one access profile ascribing read/write access to data stored on said security partition, and the other access profile ascribing a blocking level of access that does not permit write access to said security partition;

selectively blocking all data access between the host CPU and the security partition in accordance with the particular data access profile defined for a user effecting data access to the storage device at any particular point in time; and

imposing and continuously maintaining the requisite level of data access to said security partition for users effecting said data access in accordance with the particular data access profile thereof regardless of the subsequent operations of the host CPU.

17. A method as claimed in claim 16, including authenticating a user of the computer having a prescribed data access profile and configuring blocking of data access to the storage device to control subsequent access to the security partition in accordance with the data access profile of that user, before that

user is able to access said security partition regardless of the particular data access profile of that user.

18. A method as claimed in claim 16 or 17, wherein said selective blocking comprises controlling access between the host CPU and the security partition independently of the host CPU.

19. A method as claimed in claim 18, wherein said selective blocking comprises totally blocking data access to the storage device by the host CPU during initialisation of the computer and includes intercepting all said data access during the start up sequence immediately after said initialisation and before loading of the operating system of the computer, and effecting data access to the storage device and said security partition in accordance with the data access profile of users effecting said data access on authentication thereof.

20. A method as claimed in claim 19, including performing a software boot of the computer after correct authentication of the user, and allowing normal loading of the operating system during the start up sequence of the computer thereafter.

21. A method as claimed in any one of claims 17 to 20, including controlling blocking access to the storage device after correct authentication of the user in accordance with the prescribed data access profile of the user.

22. A method as claimed in any one of claims 16 to 21, including unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

23. A method as claimed in any one of the preceding claims as dependent on claim 17, wherein said authenticating includes enabling a user of the computer to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

24. A method as claimed in claim 23, wherein said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

25. A method as claimed in any one of claims 16 to 24, wherein the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions of the storage device.

26. A method as claimed in claim 25, wherein the prescribed partitions include the security partition.

27. A security system for an operating system of a computer, the security system being substantially as herein described with reference to the accompanying drawings as appropriate.

28. A method for securing and protecting an operating system of a computer from unauthorised access, substantially as herein described with reference to the accompanying drawings as appropriate.